

# TRAITE DE COOPERATION EN MATIERE DE BREVETS

## PCT

### RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire	<b>POUR SUITE A DONNER</b> voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/PEA/416)	
Demande internationale No. PCT/FR 03/01535	Date du dépôt international (jour/mois/année) 21.05.2003	Date de priorité (jour/mois/année) 05.06.2002
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.



2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

- ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :

- I ☒ Base de l'opinion
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☐ Irrégularités dans la demande internationale
- VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 19.12.2003	Date d'achèvement du présent rapport 10.11.2004
Nom et adresse postale de l'administration chargée de l'examen préliminaire international  Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé Holper, G N° de téléphone +31 70 340-2304 

PCT/FR 03/01535

**RAPPORT D'EXAMEN  
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n°

PCT/FR 03/01535

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

*(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport.)*

6. Observations complémentaires, le cas échéant :

**V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration**

1. Déclaration			
Nouveauté	Oui:	Revendications	1-14
	Non:	Revendications	
Activité inventive	Oui:	Revendications	3-7, 9
	Non:	Revendications	1,2,8,10-14
Possibilité d'application industrielle	Oui:	Revendications	1-14
	Non:	Revendications	

2. Citations et explications

**voir feuille séparée**

**Concernant le point V****Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration**

Il est fait référence aux documents suivants :

D1: US-B-6 215 872 B1 (VAN OORSCHOT PAUL C) 10 avril 2001 (2001-04-10)

D2: EP-A-0 856 821 (NIPPON TELEGRAPH & TELEPHONE) 5 août 1998 (1998-08-05)

La présente demande ne remplit pas les conditions énoncées dans l'article 33(1) PCT, l'objet des revendications 1,2, 8, 11-14 n'impliquant pas une activité inventive telle que définie par l'article 33(3) PCT.

Le document D1, qui est considéré comme étant l'état de la technique le plus proche de l'objet de la revendication 1, décrit ( voir col.4, l.11-42; col.5, l.2-5; col.8, l.60 - col.9, l.12; les références entre parenthèses s'appliquent à ce document) :

un procédé de vérification d'une signature électronique, faisant intervenir un utilisateur comprenant un système de traitement de données , l'utilisateur recevant du système de traitement de données, des demandes de vérification de signatures électroniques et traitant ces demandes, une signature électronique étant générée à l'aide d'une clé privée connue seulement d'une entité signataire et associée à une clé publique, comprenant une étape de stockage dans une table de certificats (trusted public key list 36) contenant une forme condensée d'au moins une clé publique, et une phase de vérification d'une signature électronique comportant les étapes consistant à : - recevoir la signature électronique à vérifier et une clé publique d'une paire de clés comprenant une clé privée ayant été utilisée pour générer la signature électronique à vérifier, - calculer une forme condensée de la clé publique reçue, et rechercher dans la table de certificats (36) la forme condensée calculée de la clé publique, et - déchiffrer la signature électronique à l'aide de la clé publique reçue si la forme condensée calculée de la clé publique se trouve dans la table de certificats.

Par conséquent, l'objet de la revendication 1 diffère de ce procédé connu uniquement en ce que le procédé fait intervenir un microcircuit connectable à un système de traitement de données et en ce que la table de certificats est stockée dans une mémoire du microcircuit.

Le problème que se propose de résoudre la présente invention comme définie par la revendication 1 peut donc être considéré comme étant la réalisation pratique du procédé connu.

Toutefois il est connu de stocker des certificats et des clés publiques dans une

mémoire d'une carte à puce (voir D2, fig.4B, col.5, l.57 - col.6, l.29). L'homme de l'art utiliserait sûrement une telle carte pour réaliser le procédé selon D1 et arriverait ainsi à l'objet de la revendication 1 sans exercer une activité inventive.

Le même argument s'applique mutatis mutandis à l'objet des revendications indépendantes correspondantes 13 et 14 qui ne sont donc pas non plus inventives.

La revendication dépendante 2 ne contient aucune caractéristique additionnelle qui en combinaison avec la revendication 1, définisse un objet qui satisfasse aux exigences de l'article 33(3) PCT pour la raison suivante:

les étapes supplémentaires mentionnées sont équivalentes à une vérification classique d'un certificat reçu; l'homme de l'art effectuerait cette procédure avant l'insertion d'une clé publique ou de son condensé afin de garantir l'authenticité du certificat reçu et arriverait ainsi à la matière de la revendication 2 sans exercer une activité inventive.

Les revendications dépendantes 8, 10, 11 et 12 ne contiennent aucune caractéristique qui, en combinaison avec celles de l'une quelconque des revendications à laquelle elles se réfèrent, définisse un objet qui satisfasse aux exigences du PCT en ce qui concerne l'activité inventive, voir documents D1 et D2 et les passages correspondants cités dans le rapport de recherche.

La combinaison des caractéristiques de la revendication 3 n'est pas comprise dans l'état de la technique et n'en découle pas de manière évidente pour les raisons suivantes : aucun document de l'art antérieur ne divulgue l'insertion d'un pointeur vers le condensé de la clé publique de l'entité de certification ayant émis un certificat, définissant ainsi un arbre de certification stocké dans une mémoire d'un microcircuit. La combinaison des caractéristiques de la revendication 9 n'est pas non-plus comprise dans l'état de la technique et n'en découle pas de manière évidente.

La revendications 3 et 9 remplissent donc les critères de l'article 33(2) et (3) du PCT.

Les revendications 4 - 6, en supposant qu'elles dépendent de la revendication 3, satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans les documents D1 et D2 et ne cite pas ces documents.